Report
on the examination of the design of a subsystem in the safety system “ETT Energize to Trip”

Test laboratory  TÜV SÜD Industrie Service GmbH
Abteilung Feuerungs- und Wärmetechnik
Prüfbereich Feuerungsanlagen und Thermoprozesstechnik

Subject of test  Design of a subsystem in the safety system “ETT Energize to Trip” for safety applications in FPSO (oil production ship)

Customer  Siemens AG
Process Industries and Drives
Process Automation
PD PA S AE BD
Gleiwtitzer Str. 555
90475 Nürnberg, Germany

Scope  Design examination

Expert  Dipl.-Ing. Volker Schulz

Period of test  September 2014 – December 2014

Basis of test  DIN EN 61511-1:2005, paragraph 11
This test report is also issued in a German version. In any case of doubt the German version is binding.
1 Scope

The plan is to use the safety system "ETT Energize to Trip" on FPSO (oil production ship).
In a case of fire on board of a ship the safety system „ETT Energize to Trip" shall energize actuators, for example ventilation systems and smoke dampers. For this application the safety functions have to be configured on the open-circuit current principle. This means power is required to perform the safety function.
Part of the safety instrumented system is a logic system (safety-related programmable system), with a certificate for use in safety instrumented systems based on the closed-circuit current principle (De-energizes-to-trip). Additional measures are necessary that safety functions with safety integrity level (SIL) 3 according to DIN EN 61511-1 can be performed in the planned safety instrumented system „ETT Energize to Trip".
The customer Siemens AG applied to examine the provided documentation of a subsystem inside the safety instrumented system „ETT Energize-to-trip" and define measures for the interface.
The examination of the subsystem integrated in the safety instrumented system is limited to the relevant chapter of the phase „Safety instrumented system SIS design and engineering" of the safety live-cycle according to DIN EN 61511-1.

2 Basis of test

The customer agreed that the basis of the test was DIN EN 61511-1:2005-05 chapter 11 insofar as relevant and applicable. See also chapter 5 of this test report.

3 Test documentation

- ETT FMEA V3.0 09/2014.
- Annex 1 of the test report no. SN73321C-A1 rev. 3.2 dated 2014-09-05 from TÜV SÜD Rail GmbH and certificate no. Z10 09 07 67803 004 from TÜV SÜD Product Service GmbH.
- Further documents see ETT Safety Manual chapter 7 „References“.

4 Description of the test object

The planned safety instrumented system „ETT Energize-to-trip" consists of the following three modules and the necessary sensors.
Module 1: Main power supply 1 and 2 as well as control and monitoring equipment HMI
Module 2: H-System with safety-related programmable system and I/O-Modules
Module 3: Actuators with contactors

The examination is related to subsystem module 2, which consists of the H-System with safety-related programmable system and I/O-Modules. Particulary the designed hardware components including the electrical connections and the interface to the modules 1 und 3 have to be evaluated.
The evaluation of the suitability of the designed hardware components and the connections inside the modules 1 and 3 are not in the scope this examination. This test report fixes the safety relevant measures for the interface from the modules 1 and 3 to module 2 for a later realisation.

The evaluation of the suitability and the connection of the planned sensors with the input module of the safety-related programmable system of the module 2 as well as the application logic in the safety-related programmable system of the module 2 are not in the scope of this examination. This has to be evaluated separate during the overall planning of the safety instrumented system „ETT Energize-to-trip“.

Overview of the modules and hardware components

4.1 Description of the module 1 „main power supply 1 and 2 as well as the HMI“

The power supply is ensured by two independent main power supplies.
4.2 Description of the module 2 „H-system“

The module 2 "H-system" consists of 2 redundant safety-related programmable systems S7-400H rack 0 und rack 1 as well as a redundant ET200M I/O device with an IM153-2 device and with F-DO10 output module. The communication between the safety-related programmable systems and the I/O modules has to be performed by PROFIsafe bus DP.

The safety function will be activated if at least one output channel from one of the two F-DO10 energize the contactors K1 or K2 in the module 3. This means that minimum one of the two contactors will be energized ("Energize-to-trip"). The output channel of the F-DO10 be positioned to "TRUE".

4.3 Description of the module 3 „contactors and actuators“

Via the output channel of the output module F-DO10 the actuators will be energized by the connectors K1 and K2.
5 Performance of examination

The evaluation of the design of the subsystem module 2 “H-system” inside the safety instrumented system “ETT Energize-to-trip” was performed based on the following requirements of DIN EN 61511-1:2005

- Chapter 11.2.11 “Loss of power”
- Chapter 11.3.1 “Requirements for system behaviour on detection of a fault”
- Chapter 11.4 “Hardware fault tolerance”
- Chapter 11.5 “Requirements for the selection of components and subsystems”
- Table 3 “Safety integrity levels: probability of failure on demand”

6 Results of the examination

6.1 Loss of power, DIN EN 61511-1, chapter 11.2.11

The requirements referring to DIN EN 61511-1, chapter 11.2.11 “loss of power” are fulfilled, because the power supply is ensured by two independent main power supplies.

A further evaluation of the main power supply in the module 1 “main power supply 1 and 2 and control and HMI” is not in the scope of this examination and has to be evaluated separate during the overall planning of the safety instrumented system „ETT Energize-to-trip”.

The following measures have to be considered by the total planning of the safety instrumented system „ETT Energize-to-trip“:

- The absence of interaction between the components inside the module 1 has to be ensured. A failure of a power supply has to be shown on the HMI device.
- The schematic diagram figure 2-2 referring to the safety manual ETT has to be considered.

6.2 Requirements for system behaviour on detection of a fault, DIN EN 61511-1, chapter 11.3.1

A FMEA was provided for the module 2, see annex A2. The FMEA was evaluated by the test laboratory. The FMEA take the relevant faults into account in a sufficient way.

The requirements referring to DIN EN 61511-1, chapter 11.3.1 „Requirements for system behaviour on detection of a fault” are fulfilled. In the FMEA the following faults

- Failure of the power supply
- Short circuit, wire break and overvoltage
- Failure of an F-CPU
- Failure of the IM 153-2
- Failure, passivation of the F-DO

are detected and the safety function is maintained in a single mode by the redundant architecture.
The following measures have to be considered by the overall planning of the safety instrumented system „ETT Energize-to-trip“:
- The schematic diagrams figure 2-4 and 2-5 referring to the safety manual ETT have to be considered.
- For the choice of actuators the technical connection data of the F-DO10xDC24V have to be considered.
- The readback signals of the contactors K1 and K2 are retrieved via auxiliary contacts „Feedback“.
- The suitability and the connection of the contactors and the actuators in the module 3 have to be assessed based on the requirements of DIN EN 61511-1.

6.3 Requirements for the selection of components and subsystems, DIN EN 61511-1, chapter 11.5

The planned hardware components are assessed for the use in safety applications up to SIL 3 according IEC 61508-1:1998, IEC 61508-2:2000, IEC 61508-3:1998 (see certificate no. Z10 09 07 67803 004 dated 2009-07-20 of TÜV SÜD Product Service and test report no. SN73321 C from TÜV SÜD Rail GmbH dated 2014-09-05). The relevant requirements of DIN EN 61511-1, chapter 11.5.2.1 „requirements of selected components and subsystems“ are fulfilled.

In the safety manual ETT referring chapter 2.4.1 an exemplary selection of hardware components with item numbers of the manufacturer of the safety-related programmable systems and the I/O-Modules is listed. The selection of the components has to be carried out on the basis of the annex A1 of the test report no. SN73321 CA1 dated 2014-09-05.

The following measures have to be considered by the overall planning of the safety instrumented system „ETT Energize-to-trip“:
- The measures of the certification of the safety-related programmable systems according to the test report no. SN73321 C of TÜV SÜD Rail GmbH dated 2014-09-05 have to be fulfilled.
- The components have to be selected according to annex A1 of the test report no. SN73321 CA1 dated 2014-09-05.
- The configuration and parametrization of the CPU and the F-DO10 have to be performed referring to the safety manual ETT chapter 2.5.
- The schematic diagram figure 2-3 referring to the safety manual ETT has to be considered.

6.4 Hardware fault tolerance, DIN EN 61511 chapter 11.4

On the basis of the redundant architecture of the safety system a classification up to SIL 3 according to DIN EN 61511-1, chapter 11.4.2, table 5, with SFF > 90 % and a minimum hardware fault tolerance of 1 is possible. The measures for the interfaces to the modules 1 and 3 have to be considered later by the overall planning of the safety instrumented system „ETT Energize-to-trip“:

During the later overall planning of the safety instrumented system „ETT Energize-to-trip“ the relevant requirements for the sensors and the actuators according to DIN EN 61511-1 have to be considered.
6.5 Probability of failure on demand (PFD),
DIN EN 61511-1:2003, table 3

Only the logic system including the output modules are in the scope of this evaluation.

For the PFD Value
- of the CPU 416-5H PN/DP the following value is declared by the manufacturer: < 1,9E-04
- of the output module F-DO10 the following value is declared by the manufacturer < 1,00E-05

For the PROFI safe communication the probability of a dangerous transmission error for digital communication processes $P_{TE}$ is considered once in the calculation with $P_{TE} = 10^{-5}$.

The conditions to fulfill the relevant requirements of DIN EN 61511-1, table 3, for safety function with SIL 3 are given (see certificate no. Z10 09 07 67803 004 dated 2009-07-20 from TÜV SÜD Product Service with the test report no. SN73321 C from TÜV SÜD Rail GmbH dated 2014-09-05).

For the design of the complete safety instrumented system „ETT Energize-to-trip“ consisting of

- Sensors + input module
- Logic system + output module
- Contactors + Actuators

It shall be considered that during the overall planning the calculated probability of failure on demand (PFD) has to fulfill the relevant requirements of DIN EN 61511-1, table 3 for safety functions with SIL 3.

6.6 Others

6.6.1 Sensors

The sensors have to be connected referring to the relevant connecting diagrams for safety function SIL 3 according to the Siemens safety manual for safety-related programmable systems, see certificate no. Z10 09 07 67803 004. The relevant requirements of DIN EN 61511-1 have to be fulfilled.

6.6.2 Actuators and contactors

The actuators including the contactors have to be connected referring to the relevant connecting diagrams for safety functions SIL 3 according to the Siemens safety manual for safety-related programmable systems, see certificate no. Z10 09 07 67803 004. The relevant requirements of DIN EN 61511-1 have to be fulfilled.

6.6.3 Application logic

The application logic has to fulfill the relevant requirements for safety functions SIL 3 according to the Siemens safety manual for safety-related programmable systems, see certificate no. Z10 09 07 67803 004. The relevant requirements of DIN EN 61511-1 have to be fulfilled.
7 Summary

The design of the subsystem inside the instrumented system „ETT Energize-to-trip“ in FPSO (oil production ship) to activate the safety function on the open-circuit current principle fulfils the requirements of DIN EN 61511-1, chapter 11 if the measures in the chapter 8 of this test report are considered.

For the later design of the complete instrumented system „ETT Energize-to-trip“ the measures in chapter 9 have to be considered additional.

8 Measures for the module 2 and the interface to the modules 1 and 3

8.1 Module 1 „Main power supply 1 und 2 and HMI“

8.1.1 The power supply has to be ensured by two independent main power supplies.

8.1.2 The absence of interaction between the components inside the module 1 has to be ensured. A failure of power supply has to be shown on the HMI device.

8.1.3 The schematic diagram figure 2-2 referring to the safety manual ETT has to be considered.

8.2 Module 2 „H-system“

8.2.1 The measures of the certification of the safety-related programmable systems according to the test report no. SN73321 C of TÜV SÜD Rail GmbH dated 2014-09-05 have to be fulfilled.

8.2.2 The configuration and parametrization of the CPU and the F-DO10 have to be performed referring to the safety manual ETT chapter 2.5.

8.2.3 The components have to be selected according annex A1 of the test report no. SN73321 CA1 dated 2014-09-05.

8.2.4 The schematic diagram figure 2-3 referring to the safety manual ETT has to be considered.

8.3 Module 3 „Actuators and contactors“

8.3.1 For the choice of actuators the technical connection data of the F-DO10xDC24V have to be considered.

8.3.2 Via auxiliary contacts a readback of the signals of the contactors K1 and K2 „Feedback“ has to be ensured.

8.3.3 The schematic diagrams figure 2-4 and 2-5 referring to the safety manual ETT have to be considered.
9 Measures for the design of the complete safety instrumented system according to SIL 3

9.1 During the design of the complete safety instrumented system it has to be considered that the minimum hardware fault tolerance has to fulfill the relevant requirements of the DIN EN 61511-1 for safety function SIL 3.

9.2 For the design of the complete safety instrumented system „ETT Energize-to-trip“ consisting of
- Sensors + input module
- Logic system + output module
- Contactors + Actuators

It shall be considered that during the overall planning the calculated probability of failure on demand (PFD) has to fulfill the relevant requirements of DIN EN 61511-1, table 3 for safety function with SIL 3.

9.3 Sensors

The sensors have to be connected referring to the relevant connecting diagrams for safety function SIL 3 according to the Siemens safety manual for safety-related programmable systems, see certificate no. Z10 09 07 67803 004. The relevant requirements of DIN EN 61511-1 have to be fulfilled.

9.4 Actuators and contactors

The actuators including the contactors have to be connected referring to the relevant connecting diagrams for safety functions SIL 3 according to the Siemens safety manual for safety-related programmable systems, see certificate no. Z10 09 07 67803 004. The relevant requirements of DIN EN 61511-1 have to be fulfilled.

9.5 Application logic

The application logic has to fulfill the relevant requirements for safety functions SIL 3 according to the Siemens safety manual for safety-related programmable systems, see certificate no. Z10 09 07 67803 004. The relevant requirements of DIN EN 61511-1 have to be fulfilled.

10 Recommendation

It is recommended to test the correct function of the safety instrumented system in regular intervals, minimum once a year.

Feuerungs- und Wärmotechnik
Prüfbereich Feuerungsanlagen
und Thermoprozeßtechnik

Johannes Steiglechner
Leiter
Feuerungs- und Wärmotechnik

The Expert

Volker Schulz

Annexes: A1 safety manual ETT
A2 FMEA ETT